AiDRIAN

Revenue-generating fraud prevention

A smarter way to defend against **Account Opening** and **Account Takeover** fraud

Aidrian is a continually improving fraud solution with integrated device profiling, powered by Machine Learning (ML) and a flexible rules hub. It provides increased protection against account opening and account takeover fraud.

What can Aidrian do for your business?

1. Reduce fraud rates

Machine Learning technology can quickly analyse large amounts of data and identify patterns of fraudulent activity. By constantly learning from new data, unlike the traditional rule-based systems, it can easily **adapt to fast-changing fraud patterns and make accurate recommendations** to accept, decline, or refer a complex case for investigation.

2. Increase revenue

Declining applications from good customers can negatively impact revenue. False declines can cost businesses up to **10 times more than fraud losses.** By combining device profiling with Machine Learning Aidrian achieves optimal fraud detection accuracy and minimises false declines. Plus, the accuracy of automated decisions can significantly reduce case referrals and **safely increase application acceptance rates.**

3. Reduce manual reviews

Aidrian's fraud detection accuracy can **reduce manual reviews by up to 95%.**[1] This, in turn, drives operational efficiencies and allows fraud managers to spend more time investigating complex cases. Additionally, an intuitive case manager helps make manual reviews more efficient and provides investigators with full visibility and control.

4. Seamless customer experience

Aidrian provides a step-up in fraud detection **without creating any delay**s for customers, enabling seamless experience with **passive real-time checks**. By minimising false fraud alerts, genuine customers do not get declined and frustrated. A reduction in unnecessary identity checks speeds up decisions, helping to avoid abandoned applications.

[1] Based on an Experian case study of a large retailer in Germany.

AI empowering fraudsters

Year-on-year, organisations across many sectors face significant increases in their fraud losses.[2] Day-by-day, fraudsters become smarter and faster.

1 in 2

Financial Services organisations state a lack of device fingerprinting for fraud identification as their biggest challenge in fraud prevention.[3]

With fraud attacks becoming more complex, device data is now an essential tool to help identify between legitimate customers and fraudsters.

The fastest growing fraud attack methods in Financial Services[3]

1. Synthetic identity applications

2. Identity theft

3. Account takeover

> **1/4** of world citizens lost money to scams or identity theft in the past 12 months, resulting in financial losses estimated at **$1.026 trillion**[4]

Humans are the weakest link in cybersecurity

While traditional fraud techniques still prevail, the use of generative AI fraud is accelerating fast. It can help fraudsters write malicious code and create highly personalised and convincing messages that are tailored to wide audiences for effective social engineering. This enables cybercriminals to commit **identity and account takeover fraud at scale**.

[2] IdentityTheft.org, 2023

[3] Base: 154 EMEA & APAC decision makers at Financial Services organisations. Source: Experian research conducted by Forrester Consulting, July 2023.

[4] Base: 49,459 respondents across 43 countries. Source: The Global State of Scams 2023 Report

Organisations must enhance their defences to keep pace with the evolving technology available to fraudsters.

How can Aidrian help?

Powered by device intelligence data, Machine Learning technology and a reliable flexible rule engine, Aidrian delivers accurate fraud prevention and seamless consumer experience, while helping boost revenue and reduce costs. An intuitive case investigator, with link analysis and customisable dashboard, accelerates accurate manual reviews.

Spot fraud patterns

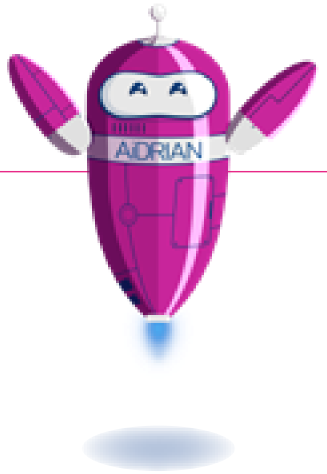
Device Profiling

Aidrian analyses multiple attributes and over 150 device data points to identify potentially fraudulent activity, and accurately assigns a Device ID.

Automate rules

Flexible Rules Hub

Create, update, and test your own rules based on current and historical transactions, and integrate custom data. Use 'silent mode' to test new rules in a live environment.



Increase revenue

Fraud Miner

A customised Machine Learning model that can tell the difference between good customers and fraudsters. Retrained every two weeks, it becomes more and more accurate over time.

Custom dashboard

Case Investigator

Access transactions for manual review with user-defined widgets and customisable dashboard. Filters, visualisations, and map view help speed up investigations.dashboard.

Machine Learning

Fraud Miner uses Machine Learning to assess application data in real-time to provide more accurate accept, refer, or decline decisions. It can **analyse millions of data points to quickly spot new fraud patterns** that are almost impossible for humans to detect.

It's a self-learning system, and is continually fed with the latest data, allowing increasingly accurate recommendations over time.

Explainability

Fraud Miner can be used in highly-regulated sectors, such as Financial Services.

78% OF FINANCIAL SERVICES ORGANISATIONS AGREE THAT

Machine Learning-based fraud detection is the most effective way of preventing fraud[5]

Independent external validation

Aidrian's Machine Learning component Fraud Miner has been validated by Fraunhofer IPA, a leading European-applied research organsiation. The audit concluded that Fraud Miner is a high-quality Machine Learning model that makes reliable predictions comprehensible to experts leading to improved decisions.

[5] Base: 154 EMEA & APAC decision makers at Financial Services organisations.
Source: Experian research conducted by Forrester Consulting, July 2023.

Device profiling

Why is device profiling important?

Device profiling can help identify when the user's device signals potentially fraudulent activity, such as identity theft. Device is remembered from the very first touchpoint and is recognised based on a specific Device ID. Device data is hard to manipulate even when the fraudster uses anonymous connection or proxy.

74% **OF FINANCIAL SERVICES ORGANISATIONS CONSIDER** device fingerprinting a must-have component of fraud prevention[6]

Examples that may indicate suspicious device activity:

- One device ID tries to log into several accounts
- Long distance between IP address location and customer's registered address
- Unusual device parameters or recent reset to factory settings
- Login via anonymous proxy

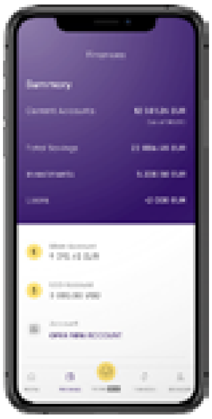
Aidrian device profiling in action

Step 1

Fraudster uses a stolen identity to apply for a credit card

Step 2

Adrian conducts a passive device check on **over 150+ parameters**



- *Operating system information*
- *Browser information*
- *Screen size and colour*
- *Browser language*
- *Time zone*
- *Device hardware details*
- *IP address and internet service provider*
- *Proxy*
- *Geo-location*
- *Http headers*

Step 3

Adrian detects device manipulations

! *Audio output not available – indication of reset device*

! *Screen size does not fit the device*

! *Anonymous VPN connection detected*

Step 4

Device identified as highly suspicious. Device ID created and blacklisted

Step 5

Fraudulent credit card application rejected

Device ID

Inability to accurately identify user's device can result in device collisions, which is one of the causes of false declines. This occurs when the same Device ID is assigned to different customers with identical devices, as they connect to the same IP address in public areas. Aidrian **avoids device collision with 99.9% accuracy**, which means a reduction in false declines, less frustrated customers and more revenue.

[6] Base: 154 EMEA & APAC decision makers at Financial Services organisations. Source: Experian research conducted by Forrester Consulting, July 2023.

Interested? Find out more.

Aidrian is a cloud-native solution with flexible APIs for rapid availability and deployment. POC available on request.

To find out more about Aidrian, contact your local Experian office or visit

experianacademy.com

Contact us